Asymptotically good towers and differential equations

Peter Beelen and Irene I. Bouw

Abstract

This paper concerns towers of curves over a finite field with many rational points, following Garcia–Stichtenoth and Elkies. We present a new method to produce such towers. A key ingredient is the study of algebraic solutions to Fuchsian differential equations modulo p. We apply our results to towers of modular curves, and find new asymptotically good towers.

1. Introduction

Let p be a prime and $q = p^a$, for some $a > 0$. Consider a projective smooth curve X of genus g, defined over $\mathbb{F}_q$, and write $N_q(X)$ for the number of $\mathbb{F}_q$-rational points of X. We write $N_q(g)$ for the maximum of $N_q(X)$, taken over all curves X of genus g which are defined over $\mathbb{F}_q$. The Drinfel'd–Vlăduţ bound [DV83] states that

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g} \leqslant \sqrt{q} - 1.$$

Moreover, $A(q) > c\log(q)$, where $c > 0$ is a constant [Ser83].

Garcia–Stichtenoth [GSR03] constructed many examples of infinite towers of curves $\cdots \to X_{m+1} \to X_m \to \cdots \to X_0$ defined over a finite field $\mathbb{F}_{q^2}$ such that the limit of $N_{q^2}(X_m)/g(X_m)$ is $q-1$. Such towers are called *asymptotically optimal*. If this limit is positive, the tower is called *asymptotically good*. Asymptotically optimal towers have, for example, interesting applications to coding theory ([Gop81, TV91]). For these applications it is important to have explicit equations for the curves X_m. Garcia–Stichtenoth define towers of curves recursively, starting from a correspondence $(g, h) : X_0 \rightrightarrows X_{-1}$, by taking suitable (normalized) Cartesian products. A nice feature of this recursive definition is that one obtains explicit equations for all curves X_m starting from an equation for (g, h). One has to choose the correspondence very carefully for the corresponding tower to have many rational points. Garcia–Stichtenoth find correspondences that work, but they do not give a systematic method for finding such correspondences.

Elkies ([Elk98]) applies this approach to correspondences $(g, h) : X_0(\ell^2) \rightrightarrows X_0(\ell)$, for certain small values of ℓ. Here g is the natural projection and h is the composition of g with the Atkin–Lehner involutions on both sides. The corresponding tower is $\cdots \to X_0(\ell^{m+1}) \to X_0(\ell^m) \to \cdots$. This gives equations for modular curves $X_0(\ell^m)$ starting from equation from $(g, h) : X_0(\ell^2) \rightrightarrows X_0(\ell)$. This is a second important application of the theory.

Elkies also constructs other asymptotically optimal towers of curves, starting from correspondences between other Shimura varieties, such as Drinfel'd modular curves. These Shimura varieties are moduli spaces of curves, surfaces etc, and the correspondences are an analog of the Hecke correspondences for modular curves. Elkies shows that all asymptotically optimal towers constructed by Garcia–Stichtenoth et. al. are of this form ([Elk98], [Elk01]). Elkies suggests that all asymptotically optimal towers arise in this way ([Elk98, Fantasia]).

2000 Mathematics Subject Classification Primary 11G20, Secondary: 14H35, 14G05, 14G50

In this paper we give a new method for constructing asymptotically good towers. We extract the essential ingredients from the approach of Garcia–Stichtenoth and Elkies, and formulate a general set-up. Our approach is concrete and not just applicable to towers of modular curves. This allows for a more systematic search for asymptotically optimal towers.

We start from a correspondence $(g,h) : X_0 \rightrightarrows X_{-1}$ over a finite field $\mathbb{F}_q$, together with a Fuchsian differential equation on X_{-1}. We say that the correspondence (g,h) is adapted to the differential equation if the pull back via g is equivalent to the pull back via h (see Section 2 for precise definitions). The correspondence (g,h) gives rise to a tower of curves $\mathcal{T}_{g,h} = (X_m)_{m\geqslant 0}$. Under some technical assumptions we show the following (Theorem 3.7).

Theorem. *The tower $\mathcal{T}_{g,h}$ is asymptotically good. This means that the limit of $N_q(X_m)/g(X_m)$ is positive.*

One of the assumptions we make is that g and h are tame, i.e. the characteristic of the ground field does not divide the ramification indices. We also give a criterion for the tower $\mathcal{T}_{g,h}$ to be asymptotically optimal (Theorem 3.8).

The reason why such towers have many rational points is roughly the following. We suppose that the differential equation has an algebraic solution Φ. After extending the field of definition $\mathbb{F}_q$ of the correspondence, we may assume that the zeros and poles of Φ are $\mathbb{F}_q$-rational. The set of these zeros and poles has a subset T with the following property. For every $P \in T$ and every m, the inverse image of P in X_m consists of unramified and $\mathbb{F}_q$-rational points.

It appears that all known examples of tame asymptotically optimal towers can be reformulated in these terms. The reason is that, by Elkies' work, the known examples come from certain correspondences between Shimura curves. (In fact, the tame towers are all towers of modular curves.) Such moduli spaces come naturally equipped with a differential equation: the Picard–Fuchs differential equation of a versal family of the objects it parameterizes. For towers of modular curves we work this out in Section 5. We expect that it is possible to generalize (parts of) our method to wildly ramified towers.

The idea for using differential equations for studying the growing behavior of rational points in a tower came from [GSR03]. In that paper Gauß' hypergeometric differential equation was used to prove a property for the Deuring polynomial. We show that the arguments of [GSR03] simplify and generalize if one makes a more systematic use of differential equations. Our method is also related in spirit to older work of Ihara (see [Iha99] for a survey). However, Ihara's work only applies to towers of Shimura curves. Moreover, it uses p-adic uniformization to count points. We work purely in characteristic p which is more convenient in practice.

To find new examples of asymptotically good towers, we construct correspondences via pull back. Given a correspondence $(g,h) : X_0 \rightrightarrows X_{-1}$ and an arbitrary map $f : Y_{-1} \to X_{-1}$, we define a new correspondence $(\tilde{g},\tilde{h}) : Y_0 \rightrightarrows Y_{-1}$. This gives a systematic construction of the towers of modular curves found by Elkies in [LMS02, Appendix]. This allows one to find many asymptotically good towers.

The situation for asymptotically optimal towers is more complicated. We give a criterion for the pull back of an asymptotically optimal tower to be again asymptotically optimal (Theorem 4.5). Since our approach does not use the interpretation of the curves we consider as Shimura varieties, one might expect to find counterexamples to Elkies' Conjecture. However, we did not find such an example. The reason is that in Theorem 4.5 there is one condition which is hard to control. In a later paper we will come back to the question whether this idea can be used as evidence for Elkies' Conjecture.

The organization of the paper is as follows. In Section 2 we review and extend known results on Fuchsian differential equations on curves in positive characteristic. In Section 3 we give the recursive definition of a tower of curves corresponding to a correspondence and establish basic properties. We estimate how the genus and the number of rational points grow in the tower, and prove the criterion for a tower to be asymptotically good. In Section 4 we develop the construction of correspondences via pull back and construct a new example. Section 5 reformulates and extends some results of Elkies on towers of modular curves.

2. Fuchsian differential equations

In this section we recall some standard results on Fuchsian differential equations. For proofs and more details we refer to [Kat70, Section 11] and [Hon81]. Let k be a field of characteristic $p > 0$ and X/k a smooth projective curve. Let $K = k(X)$ be the function field of X. Suppose that M is a finite-dimensional vector space over K.

Definition 2.1. A k-connection ∇ on M is an additive map

$$\nabla : M \to \Omega^1_{K/k} \otimes_K M$$

satisfying the Leibniz rule

$$\nabla(fm) = \mathrm{d}f \otimes m + f\nabla(m),$$

for $f \in K$ and $m \in M$.

Equivalently ([Kat70, Section 1.0]), ∇ corresponds to a K-linear map

$$\nabla : \mathrm{Der}(K/k) \to \mathrm{End}_k(M)$$

such that $\nabla(D)(fm) = D(f)m + f\nabla(D)m$ for $D \in \mathrm{Der}(K/k)$, $f \in K$ and $m \in M$. A *horizontal morphism* from (M_1, ∇_1) to (M_2, ∇_2) is a morphism $\varphi : M_1 \to M_2$ of K-vector spaces which is compatible with the connections, i.e. $\varphi(\nabla_1(D)m) = \nabla_2(D)(\varphi(m))$. We write $\mathrm{MC}(X)$ for the category of K-modules with connection.

Definition 2.2. Let P be a place of K/k and t a local parameter at P. For a K-basis $\mathbf{e}$ of M, we write $\nabla(\mathrm{d}/\mathrm{d}t)\mathbf{e} = A_{\mathbf{e}} \cdot \mathbf{e}$ with $A_{\mathbf{e}} \in M_n(K)$, where $n = \dim_K M$. We say that P is a *singular point* of (M, ∇) if the matrix $A_{\mathbf{e}}$ has a pole at P for every basis $\mathbf{e}$.

Definition 2.3. We say that (M, ∇) is *cyclic* if there exists a vector $m \in M$ and a nonzero derivation $D \in \mathrm{Der}(K/k)$ such that $m, \nabla(D)m, \ldots \nabla^{d-1}(D)m$ span M over K, where $d = \dim_K M$.

It is shown in [Kat70, 11.4] that the notion of a cyclic module is independent of the choice of the derivation D. In the rest of this section, we suppose that M is cyclic, and of K-dimension $d = 2$. A K-basis $m, \nabla(D)m$ of M is called a *cyclic basis*.

If P is place of K/k, we write $\mathcal{O}_P$ (resp. $\mathfrak{m}_P$) for the local ring (resp. the maximal ideal) at P. Let

$$\mathrm{Der}_P(K/k) = \{D \in \mathrm{Der}(K/k) \,|\, D(\mathfrak{m}_P) \subset \mathfrak{m}_P\}.$$

If $t = t_P$ is a local parameter of X at P, then $\mathrm{Der}_P(K/k)$ is a free $\mathcal{O}_P$-module with basis $t\,\mathrm{d}/\mathrm{d}t$.

Definition 2.4. Let P be a singular point of (M, ∇) and t a local parameter at P. For a K-basis $\mathbf{e}$ of M, we write $\nabla(t\,\mathrm{d}/\mathrm{d}t)\mathbf{e} = B_{\mathbf{e}} \cdot \mathbf{e}$ with $B_{\mathbf{e}} \in M_2(K)$. We say that P is a *regular singularity* if there exists a K-basis $\mathbf{e}$ of M such that $B_{\mathbf{e}}$ is holomorphic at P. If all singularities of (M, ∇) are regular, we say that (M, ∇) is a *Fuchsian module*.

Suppose that P is a regular singularity of (M, ∇), and let $B_{\mathbf{e}} \in M_n(\mathcal{O}_P)$ be as above. Write $B_{\mathbf{e}}(0)$ for the value of $B_{\mathbf{e}}$ at $t = 0$. The characteristic polynomial of $B_{\mathbf{e}}(0)$ is called the *indicial equation*. Its roots are the *local exponents*.

The local exponents depend on the choice of the basis $\mathbf{e}$. In this paper we always suppose that $\mathbf{e}$ is chosen such that the matrix of $\nabla(D)$ is regular. Here $D = t\mathrm{d}/\mathrm{d}t$ if P is a singularity and $D = \mathrm{d}/\mathrm{d}t$ otherwise. If P is not a singularity its local exponents are $0, 1 = \dim_K M - 1$. The converse need not be true. Singularities with local exponents $0, 1 = \dim_K M - 1$ are called *apparent singularities*.

We now associate to (M, ∇) a 2nd order differential equation. Let P be a regular singularity of (M, ∇) and t a local parameter at P. Let $\mathbf{e} = (e_1, e_2 := \nabla(\mathrm{d}/\mathrm{d}t)(e_1))$ be a cyclic basis of M. Write

$$\nabla(\frac{\mathrm{d}}{\mathrm{d}t})\mathbf{e} = A \cdot \mathbf{e}, \qquad \text{with} \qquad A = \begin{pmatrix} 0 & -a_2 \\ 1 & -a_1 \end{pmatrix}. \tag{1}$$

It is easy to check that the fact that P is a regular singularity means that we may choose $\mathbf{e}$ such that a_i has a pole of order at most i at P for $i = 1, 2$.

Let $M^* = \mathrm{Hom}_K(M, K)$ be the K-linear dual of M. We define a k-connection ∇^* on M^* by requiring that

$$\langle \nabla(D)(m), m^* \rangle + \langle m, \nabla^*(D)(m^*) \rangle = D(\langle m, m^* \rangle),$$

for $D \in \mathrm{Der}(K/k)$, $m \in M$ and $m^* \in M^*$. One easily checks that ∇^* is a connection. In fact, with respect to the dual basis $\mathbf{e}^*$ of M^*, we have $\nabla^*(\mathrm{d}/\mathrm{d}t)\mathbf{e}^* = -A^t\mathbf{e}^*$. Here A^t is the transpose of A.

Write $\hat{M}_P^* = M^* \otimes_K \hat{K}_P$, where $\hat{K}_P$ is the completion of K at P. Denote by $(\hat{M}_P^*)^{\nabla^*}$ the horizontal sections, i.e.

$$f_1 e_1^* + f_2 e_2^* \in (\hat{M}_P^*)^{\nabla} \qquad \text{iff} \qquad \begin{cases} f_2 = f_1', \\ L(f_1) := f_1'' + a_1 f_1' + a_2 f_1 = 0. \end{cases} \tag{2}$$

This is the *differential equation corresponding to* (M, ∇). Giving (M, ∇) is equivalent to giving the differential equation (2). We sometimes call (M, ∇) itself a differential equation.

One computes that

$$\nabla(t\frac{\mathrm{d}}{\mathrm{d}t})(e_1, te_2) = \begin{pmatrix} 0 & -t^2 a_2 \\ 1 & 1 - ta_1 \end{pmatrix} (e_1, te_2).$$

Writing $a_i = c_i t^{-i} + \cdots$ with $c_i \in \bar{k}$, we find that the indicial equation is

$$X^2 + (-1 + c_1)X + c_2 = 0. \tag{3}$$

The local exponents γ_1, γ_2 are the roots of this equation. Note that our notion of local exponents agrees with the classical ones. This is the reason for taking the differential equation corresponding to the horizontal sections of $\hat{M}_P^*$ rather than $\hat{M}_P$.

Our next topic is algebraic solutions of Fuchsian differential equations in positive characteristic, following Honda [Hon81]. Let $(M, \nabla) \in \mathrm{MC}(X)$ be a cyclic module of dimension 2, and let $P \in X$ be a regular singularity with local parameter t. Choose a cyclic basis $\mathbf{e}$ of M. Let L/K be an algebraic extension. We say that $u \in L$ is an *algebraic solution* of (M, ∇) if it is a solution of the corresponding differential equation (2). This is equivalent to the fact that $ue_1^* + u'e_2^* \in (M^* \otimes_K L)^{\nabla^*}$. In what follows we mainly consider solutions in K.

Proposition 2.5. *Let $(M, \nabla) \in \mathrm{MC}(X)$ be a cyclic module of dimension 2, and let $u \in K$ be an algebraic solution (with respect to some choice of a cyclic basis $\mathbf{e}$).*

(i) Suppose that P is a regular singularity. Write γ_1, γ_2 for its local exponents. Then

$$\mathrm{ord}_P(u) \equiv \gamma_i \bmod p,$$

for some $i \in \{1, 2\}$. In particular, $\gamma_i \in \mathbb{F}_p$.

(ii) If $P \in X$ is regular we have

$$\mathrm{ord}_P(u) \equiv 1 \bmod p \qquad \text{or} \qquad \mathrm{ord}_P(u) \equiv 0 \bmod p.$$

Proof. Let u be an algebraic solution. Suppose that P is a regular singularity. Choose a local parameter t at P. Put $\delta := \mathrm{ord}_P(u)$. In the complete local ring $\hat{\mathcal{O}}_P$, we may write $u = t^\delta(\epsilon)$ with $\epsilon \in \hat{\mathcal{O}}_P^\times$. By assumption, u satisfies

$$u'' + a_1 u' + a_2 u = 0,$$

where a_i has a pole of order at most i, since P is a regular singularity. Write

$$a_1 = c_1 t^{-1} + \cdots, \qquad a_2 = c_2 t^{-2} + \cdots.$$

Substituting this in the differential equation and taking the coefficient of $t^{\delta-2}$, we find that $\delta^2 + \delta(c_1 - 1) + c_2$. Since the indicial equation (3) is $X^2 + (c_1 - 1)X + c_2$, (a) follows.

If P is a regular point, we may suppose that a_i does not have a pole at P for $i = 1, 2$. Hence (b) immediately follows from the indicial equation. □

Example 2.6. A key example of a Fuchsian differential equation we will be interested in this paper, is the one coming from the Gauß–Manin connection on the modular curve $X(2)$. We recall the situation from [Kat84]. The statements are easy to generalize to other modular curves (Section 5). Let $S = \mathrm{Spec}(\mathbb{Z}[\lambda, 1/2\lambda(\lambda-1)])$ and write $\mathcal{E} \to S$ for the elliptic curve over S given by $y^2 = x(x-1)(x-\lambda)$.

We denote by $M := H^1_{\mathrm{dR}}(\mathcal{E}/S)$ the first de Rham cohomology group, and by $\nabla : M \to \Omega^1_S \otimes M$ the Gauß–Manin connection. Write

$$\omega = \frac{\mathrm{d}x}{y} = \frac{\mathrm{d}x}{[x(x-1)(x-\lambda)]^{1/2}}, \qquad \omega' := \nabla(\frac{\partial}{\partial\lambda})\,\omega = \frac{\mathrm{d}x}{2[x(x-1)]^{1/2}(x-\lambda)^{3/2}}.$$

Then ω and ω' form a basis of M. One computes that

$$\nabla(\frac{\partial}{\partial\lambda})(\omega,\omega') = \begin{pmatrix} 0 & -1/4\lambda(\lambda-1) \\ 1 & -(2\lambda-1)/\lambda(\lambda-1) \end{pmatrix} (\omega,\omega').$$

The corresponding differential equation (2) is

$$\lambda(\lambda-1)u'' + (2\lambda-1)u' + \frac{1}{4}u = 0. \tag{4}$$

The differential equation (4) is Gauß' hypergeometric differential equation. It has three singularities $0, 1, \infty$ with local exponents $0, 0; 0, 0; 1/2, 1/2$. Working out the statement of Proposition 2.5 for the singularity $P = \infty$, we obtain the following. Let $u \in k(\lambda)$ be an algebraic solution. After multiplying u with a pth power, we may suppose that u is a polynomial. Then $\deg(u) \equiv -\gamma_i \bmod p$, were γ_1, γ_2 are the local exponents at ∞. In our case we find therefore that $\deg(u) \equiv -1/2 \bmod p$.

The Deuring polynomial (or Hasse invariant)

$$\Phi := \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 \lambda^i \tag{5}$$

is a solution mod p of this differential equation of degree $(p-1)/2$. Proposition 2.7 below implies that every other algebraic solution in characteristic p is of the form $\psi^p\Phi$, for some $\psi \in K$.

In this paper we always assume that the K^p-module of algebraic solutions of (M, ∇) has dimension one. This restriction may not be necessary. We make it because it is always satisfied in the concrete cases we consider and significantly simplifies the exposition. This condition can be reformulated in terms of the p-curvature as follows.

The *p-curvature* of (M, ∇) is the K-linear morphism

$$\Psi_M : \mathrm{Der}(K/k) \to \mathrm{End}_K(M)$$

defined by

$$\Psi_M(D) = \nabla(D)^p - \nabla(D^p).$$

See [Kat70, Section 5] for basic properties of the p-curvature. Suppose that (M, ∇) has an algebraic solution $u \in K$. Then it is well-known that then the K^p-module of algebraic solutions of (M, ∇) has dimension one if and only if the p-curvature Ψ_M is nonzero ([Hon81, Appendix] and [Kat70, Theorem 5.1]). The following proposition gives a necessary condition for this to happen. A similar statement is proved in [Hon81, Proposition 5.1].

Proposition 2.7. *Let $(M, \nabla) \in \mathrm{MC}(X)$ be a cyclic module of dimension 2, and let $u_1, u_2 \in K$ be algebraic solutions (with respect to some choice of a cyclic basis $\mathbf{e}$). We suppose that $\mathrm{ord}_P(u_1) \equiv \mathrm{ord}_P(u_2) \bmod p$ for some regular singularity P. Then u_1 and u_2 are linearly dependent over K^p.*

Proof. Let $u_1, u_2 \in K$ be solution of the differential equation which are independent over K^p. Choose a local parameter t at P. Let $\gamma = \mathrm{ord}_P(u_1)$ and $\gamma + p\nu = \mathrm{ord}_P(u_2)$. It is no restriction to suppose that $\gamma = 0$. Write $u_1 = \sum_{i\geqslant 0} b_i t^i$ and $u_2 = t^{p\nu}(\sum_{i\geqslant 0} d_i t^i)$. It is no restriction to suppose that $b_0 = d_0 = 1$. Let $w = u_2' u_1 - u_1' u_2$ be the Wronskian; it satisfies the differential equation $w' + a_1 w = 0$.

It is easy to see that the assumption that u_1 and u_2 are independent over K^p implies that the local exponents at P are both zero. One computes that

$$w = t^{p\nu} \sum_{i\geqslant 0} \sum_{j=0}^{i+1} (i+1-2j) d_{i+1-j} b_j.$$

Since $\mathrm{ord}_P(w) \equiv -1 \bmod p$, it follows that $b_i = d_i$ for $i = 0, \ldots, p-2$. The coefficient of $t^{p(\nu+1)-1}$ in w is $p(d_p b_0 - d_0 b_p) = 0$. Continuing we find that $w = 0$. But this contradicts the assumption that the solutions u_1 and u_2 are linearly independent over K^p. □

Proposition 2.7 may also be rephrased as follows. Suppose that there exists a $P \in X$ such that the local exponents of (M, ∇) at P are equal, then the space of algebraic solution of (M, ∇) in L has L^p-dimension one.

In general, a module $(M, \nabla) \in \mathrm{MC}(X)$ does not have algebraic solutions. Honda [Hon81, appendix] shows that (M, ∇) has "sufficiently many solutions in a weak sense" if and only if the p-curvature of (M, ∇) is nilpotent. The notion of sufficiently many solutions in a weak sense is stronger than just the existence of an algebraic solution, namely one requires that the Wronskian equation $w' + a_1 w = 0$ has a nonzero algebraic solution as well. However, if (M, ∇) is cyclic, has dimension two, and its singularities are $\mathbb{F}_p$-rational than the two notions are equivalent [Hon81, Cor. 1 to Prop. 2.3]. Katz [Kat70] shows that in a "geometric" context (like in Example 2.6) the p-curvature is always nilpotent, in particular, the corresponding differential equation has an algebraic solution in some extension L/K.

Suppose that (M_1, ∇_1) and (M_2, ∇_2) are elements of $\mathrm{MC}(X)$. We define a k-connection ∇ on $M = M_1 \otimes_K M_2$ by putting $\nabla(D)(m_1 \otimes m_2) = (\nabla_1(D)m_1) \otimes m_2 + m_1 \otimes (\nabla(D)m_2)$, for $D \in \mathrm{Der}(K/k)$ and $m_i \in M_i$.

Definition 2.8. Let (M_1, ∇_1), $(M_2, \nabla_2) \in \mathrm{MC}(X)$ be modules with $\dim_K M_1 = \dim_K M_2$. We say that (M_1, ∇_1) is *equivalent* to (M_2, ∇_2) if there exists a one-dimensional module $(M_3, \nabla_3) \in \mathrm{MC}(X)$ such that:

- $(M_1, \nabla_1) \otimes_K (M_3, \nabla_3) \simeq (M_2, \nabla_2)$,
- (M_3, ∇_3) has an algebraic solution θ,
- the set of singularities of (M_3, ∇_3) is contained in the set of singularities of (M_1, ∇_1).

In terms of local coordinates this definition means the following. Let $(M_1, \nabla_1) \in \mathrm{MC}(X)$ be a cyclic, Fuchsian module of dimension two and let $(M_3, \nabla_3) \in \mathrm{MC}(X)$ be a one-dimensional Fuchsian module. Let P be a regular singularity of both (M_1, ∇_1) and (M_3, ∇_3) with local parameter t. Choose a cyclic basis (e_1, e_2) for M_1 as in (1), i.e. we write

$$\nabla_1(\mathrm{d}/\mathrm{d}t)(e_1, e_2) = \begin{pmatrix} 0 & -a_2 \\ 1 & -a_1 \end{pmatrix} (e_1, e_2).$$

We identify M_3 with K, and write $\nabla_3(\mathrm{d}/\mathrm{d}t) = B \cdot 1$. Then with respect to the basis $\xi_1 = e_1 \otimes 1$ and $\xi_2 = Be_1 \otimes 1 + e_2 \otimes 1$ of $M_2 = M_1 \otimes_K M_3$ we find

$$\nabla_2(\mathrm{d}/\mathrm{d}t)(\xi_1, \xi_2) = \begin{pmatrix} 0 & -a_2 + Ba_1 + B' - B^2 \\ 1 & -a_1 + 2B \end{pmatrix} (\xi_1, \xi_2).$$

The corresponding differential equation is

$$y'' + (a_1 - 2B)y' + (-B' - Ba_1 + a_2 + B^2)y = 0.$$

One checks that if u is an (algebraic) solution of the differential equation corresponding to (M_1, ∇_1) then θu is an (algebraic) solution of (M_2, ∇_2). Here θ is an algebraic solution of M_3 (Definition 2.8). Let γ (resp. γ_1, γ_2) be the local exponents of (M_3, ∇_3) (resp. (M_1, ∇_1)) at P. One computes that the indicial equation of (M_2, ∇_2) at P is $(X - \gamma_1 - \gamma)(X - \gamma_2 - \gamma)$.

Suppose we are given $(M, \nabla) \in \mathrm{MC}(X)$ and a cover $f : Y \to X$ defined over k, i.e. f is a finite separable map between smooth and absolutely irreducible curves. Let $L = k(Y)$ be the function field of Y.

Definition 2.9. We define the *pull back* (M_f, ∇_f) on Y as follows. Write $\nabla(m) = m \otimes \mathrm{d}g$, where $\mathrm{d}g \in \Omega^1_K$. Then $M_f = M \otimes_K L$ and $\nabla_f : M \otimes_K L \to \Omega^1_L \otimes (M \otimes_K L)$ is defined by $m \otimes 1 \mapsto f^*(m \otimes \mathrm{d}g) := m \otimes \mathrm{d}(g \circ f) \in M \otimes_K L \otimes_L \Omega^1_L = M_f \otimes_L \Omega^1_L$.

In local coordinates this may be described as follows. Let Q be a point of Y and P its image in X. Choose a local parameter s of Q and let $t = s^e$ be a local parameter of P. Here e is the ramification index of Q in f. Write $f'(s) \in \mathcal{O}_Q$ for the derivative of f at Q. Choose an appropriate basis $\mathbf{e} = (e_1, e_2)$ of M at P, and write

$$\nabla(\mathrm{d}/\mathrm{d}t)\mathbf{e} = \begin{pmatrix} 0 & -a_2 \\ 1 & -a_1 \end{pmatrix} \mathbf{e},$$

as above. Then

$$\nabla_f(\mathrm{d}/\mathrm{d}s)(e_1, f'(s)e_2) = \begin{pmatrix} 0 & -(f'(s))^2 a_2(f(s)) \\ 1 & -f'(s)a_1(f(s)) + f''(s)/f'(s) \end{pmatrix} (e_1, f'(s)e_2).$$

The corresponding differential equation is

$$L_f(v) = \left(\frac{\mathrm{d}}{f'(s)\mathrm{d}s}\right)^2 v + a_1(f(s)) \left(\frac{\mathrm{d}}{f'(s)\mathrm{d}s}\right) v + a_2(f(s))v = 0.$$

One easily checks that if (M, ∇) is Fuchsian, then (M_f, ∇_f) is Fuchsian also. Moreover, with notation as above, if P is a regular singularity with local exponents (γ_1, γ_2) then $(e\gamma_1, e\gamma_2)$ are the local exponents at Q. Note that it may happen that P is a singularity but Q is not. (It is easy to characterize this in terms of the local monodromy, but we do not need this here.)

Notation 2.10. Let $(M, \nabla) \in \mathrm{MC}(X)$ and write S for its set of singularities. Suppose that (M, ∇) has an algebraic solution Φ. Let $f : Y \to X$ be a cover and (M_f, ∇_f) the pull back module. We write $\Phi_f := \Phi \circ f$ for the corresponding algebraic solution of (M_f, ∇_f).

Definition 2.11. Let $(M, \nabla) \in \mathrm{MC}(X)$. A *correspondence adapted to* (M, ∇) is a pair of (separable) covers $g, h : Y \rightrightarrows X$ between smooth and absolutely irreducible curves such that the pull back modules (M_g, ∇_g) and (M_h, ∇_h) on Y are equivalent. A correspondence (g, h) is called *tame* if the covers g and h are tame.

A correspondence $(g, h) : Y \rightrightarrows X$ may equivalently be described by giving a curve $C \subset X \times X$. Here $C = \{(g(P), h(P)) \,|\, P \in Y\}$ is the *curve of correspondence*. The *degree of the correspondence* is the cardinality of $\{(x, y) \in C\}$, where $x \in X$ is a fixed, sufficiently general point. We will be particularly interested in correspondences of degree one. In this case the map $Y \to C$ defined by $P \mapsto (g(P), h(P))$ is generically an isomorphism.

Proposition 2.12. *Let $(M, \nabla) \in \mathrm{MC}(X)$ be a Fuchsian, cyclic module of dimension two. Let S be its set of singularities. Suppose that*

- *(M, ∇) has an algebraic solution $\Phi \in K$, and*
- *the p-curvature of (M, ∇) is nilpotent, but nonzero.*

Let $(g, h) : Y \rightrightarrows X$ be a correspondence adapted to (M, ∇). Write $\mathfrak{S}$ for the set of singularities of the pull back module (M_g, ∇_g). Then there exists a function $\epsilon \in K(Y)$ and a function $\theta \in K(Y)$ whose poles and zeros are contained in $\mathfrak{S}$ such that

$$\Phi_h = \epsilon^p \theta \Phi_g.$$

Proof. Note that $\mathfrak{S}$ is also the set of singularities of (M_h, ∇_h). The fact that (M_g, ∇_g) and (M_h, ∇_h) are equivalent means that there exists a one-dimensional module (N, ∇_N) such that $(M_g, \nabla_g) \otimes (N, \nabla_N) \simeq (M_h, \nabla_h)$. It is no restriction to suppose that we have equality. Recall that there exists an algebraic function θ such that $\theta\Phi_g$ is a solution of (M_h, ∇_h). This function is an algebraic solution of the module (N, ∇_N).

Theorem 5.9 of [Kat70] implies that the p-curvature of the pull back modules (M_h, ∇_h) is nilpotent as well. It follows from the interpretation of $\Psi_M = 0$ in terms of algebraic solutions that $\Psi_{M_h} \neq 0$. Since $\theta\Phi_g$ and Φ_h are both solutions of (M_h, ∇_h), it follows that they differ by an element of $K(Y)^p$. □

Lemma 2.13. *Let $(M, \nabla) \in \mathrm{MC}(X)$ and $g, h : Y \rightrightarrows X$ be a correspondence adapted to (M, ∇). Then, for every map $\phi : Z \to Y$, the modules $(M_{g\circ\phi}, \nabla_{g\circ\phi})$ and $(M_{h\circ\phi}, \nabla_{h\circ\phi})$ are equivalent also.*

Proof. Straightforward. □

3. Estimates for the number of points and the genus in a tower

In this section we define a tower of curves from a tame correspondence adapted to a differential equation (M, ∇). We also estimate the genus (Proposition 3.3) and number of points (Proposition 3.6) in the tower. The results are easiest to understand in the well-known case of towers of modular curves (Section 5). It may be helpful to look at this case before reading the proofs in the general case.

Let (M, ∇) be a Fuchsian differential equation of rank 2 with set of singularities S. We always suppose that M is cyclic (Definition 2.3). We denote by $(g, h) : X_0 \rightrightarrows X_{-1}$ a tame correspondence adapted to (M, ∇) (Definition 2.11) unbranched outside S. We always assume that X_0 and X_{-1} are smooth and absolutely irreducible curves. We assume that the covers g and h are disjoint (i.e. the covers $g, h : X_0 \to X_{-1}$ do not have a common subcover, or alternatively, there do not exist functions ϕ, ψ_1 and ψ_2 such that $g = \phi \circ \psi_1$ and $h = \phi \circ \psi_2$ and $\deg \phi \neq 1$). Denote the common set of singularities of (M_g, ∇_g) and (M_h, ∇_h) by $\mathfrak{S}$. To the correspondence (g, h) we associate a tower of curves

$$\mathcal{T}_{g,h} = \left(\cdots \xrightarrow{\pi_m} X_m \xrightarrow{\pi_{m-1}} X_{m-1} \to \cdots \xrightarrow{\pi_0} X_0 \right), \tag{6}$$

where X_m is a smooth projective curve and π_m is a cover. For $m \geqslant 1$, the curve X_m is the normalization of the curve X'_m. The curves X'_m are defined recursively as follows. We put $X'_0 = X_0$. For $m \geqslant 0$, we define X'_{m+1} by the fiber product

$$\begin{tikzcd} X'_{m+1} \arrow[r] \arrow[d, "\pi_m"'] & X_0 \arrow[d, "h"] \\ X'_m \arrow[r, "g_m"'] & X_{-1}, \end{tikzcd}$$

where $\pi_m(x_0, \dots, x_{m+1}) = (x_0, \dots, x_m)$ and $g_m(x_0, \dots, x_m) = g(x_m)$. We have

$$X'_m = \{(x_0, \dots, x_m) \in X_0^{m+1} \,|\, h(x_i) = g(x_{i-1}),\ 1 \leqslant i \leqslant m\}.$$

The cover $\pi_m : X'_{m+1} \to X'_m$ induces a cover from X_{m+1} to X_m which we again denote by π_m. We will also denote by $x_i : X_m \to X_0$ (with $0 \leqslant i \leqslant m$) the cover defined by $x_i : P \mapsto x_i(P)$.

To obtain a tower of curves, we require that X_m is an absolutely irreducible curve, for all m. Clearly, a necessary condition for this is that g and h are disjoint. This condition is not sufficient however. For example if we take $g(t) = t^2 + t$ and $h(t) = 1/(t^2 + t)$ both defined over a finite field of characteristic two, then g and h are disjoint, but the corresponding curve X_2 is not irreducible (although X_1 is).

We now state a sufficient condition for all curves X_m occurring in the tower $\mathcal{T}_{g,h}$ to be absolutely irreducible. Let Y and X be curves defined over a field k and suppose we are given a cover $\pi : Y \to X$ defined over k. We say a point P of X is *totally branched* in the cover π if there exists a point Q of Y with $\pi(Q) = P$ such that $e(Q|P) = \deg \pi$. The following lemma is obvious.

Lemma 3.1. *Suppose that the cover $\pi_m : X_{m+1} \to X_m$ has a totally branched point for all $m \geqslant 0$. Then all curves X_m are absolutely irreducible.*

The condition that g and h are disjoint is not vital for the construction of the tower. If $g = \phi \circ \psi_1$ and $h = \phi \circ \psi_2$, one should replace the correspondence (g, h) by (ψ_1, ψ_2). Note that if g and h are disjoint we have $\deg \pi_m = \deg h$. All asymptotically good towers of function fields found by Garcia–Stichtenoth et al. (see e.g. [GS95, GSR03, GS96, GST97]) can be described as a tower $\mathcal{T}_{g,h}$ for a suitable correspondence (g, h). For the definition of the tower, we do not need that the correspondence is adapted to some differential equation. We only need this afterwards to estimate the number of $\mathbb{F}_q$-rational points.

We now state some restrictions we will assume in the rest of this section.

Assumption 3.2. Let $(g, h) : X_0 \rightrightarrows X_{-1}$ be a tame correspondence adapted to a Fuchsian, cyclic module (M, ∇) of rank 2.

(a) The set of singularities $S \subset X_{-1}$ of (M, ∇) contains the branch locus of g and h.
(b) $\mathfrak{S} = g^{-1}(S) = h^{-1}(S)$.
(c) All curves X_m occurring in the tower $\mathcal{T}_{g,h}$ are absolutely irreducible.
(d) $\deg g = \deg h =: \delta$.
(e) The module (M, ∇) has an algebraic solution $\Phi \in K$ and $\Psi_M \neq 0$.

We will usually check (c) by using Lemma 3.1. Note that (d) is a natural restriction, since if $\deg g \neq \deg h$ the tower $\mathcal{T}_{g,h}$ is asymptotically bad [GS00].

We start by estimating the genus $g(\mathcal{T}_{g,h})$ of a tower $\mathcal{T}_{g,h}$. This genus is defined in the following way:

$$g(\mathcal{T}_{g,h}) := \lim_{m\to\infty} \frac{g(X_m)}{\delta^m}.$$

Here $g(X_m)$ denotes the genus of the curve X_m. This limit exists [GST97], but may be infinite. A necessary condition for a tower $\mathcal{T}$ to be asymptotically good is that $0 < g(\mathcal{T}) < \infty$. The following proposition checks this in our situation.

Proposition 3.3. *Suppose Assumption 3.2 holds. Then for any m and any point P of X_m we have*

i) $x_{m-1}(P) \in \mathfrak{S} \Longleftrightarrow x_m(P) \in \mathfrak{S}$,

ii) $g(\mathcal{T}_{g,h}) \leqslant g(X_0) + \frac{\#\mathfrak{S}-2}{2}$.

Proof. We extend the constant field to $\overline{\mathbb{F}}_q$, which does not make a difference since we are only interested in the genus at this point. We show that the branch locus of the tower $\mathcal{T}_{g,h}$ is contained in $\mathfrak{S}$. (By branch locus we mean here the set of points of X_0 that are branched in the cover $X_m \to X_0$, for some m.)

Let P be a point of the curve X_m. By the recursive definition of the tower, we have $h(x_m(P)) = g(x_{m-1}(P))$. Therefore, if $x_{m-1}(P) \in \mathfrak{S}$, we have $x_m(P) \in h^{-1}g(x_{m-1}(P)) \subset h^{-1}g(\mathfrak{S}) = \mathfrak{S}$ by Assumption (b). Conversely, $x_m(P) \in \mathfrak{S}$ implies $x_{m-1}(P) \in \mathfrak{S}$. This proves the first part of the proposition.

Recall that the following diagram commutes

$$\begin{tikzcd} X_m \arrow[r] \arrow[d, "\pi_{m-1}"'] & X_0 \arrow[d, "h"] \\ X_{m-1} \arrow[r, "g_{m-1}"'] & X_{-1}. \end{tikzcd}$$

If $P \in X_m$ ramifies in $\pi_{m-1} : X_m \to X_{m-1}$ then $g(x_{m-1}(P)) \in S$, since we assumed that h is unbranched outside S. By assumption (b), we have that $x_m(P) \in \mathfrak{S}$. It follows by induction from part i) that $x_0(P) \in \mathfrak{S}$.

One uses the Riemann–Hurwitz formula for the cover $X_m \to X_0$ to deduce

$$\frac{g(X_m)-1}{\delta^m} \leqslant g(X_0) - 1 + \frac{\#\mathfrak{S}\cdot(\delta^m - 1)}{2\delta^m}.$$

The proposition follows by letting m tend to infinity. □

We now investigate the asymptotic behavior of the number of rational points in the tower $\mathcal{T}_{g,h}$. A key role is is played by Proposition 2.12. Let Φ be an algebraic solution of (M, ∇). Further, let Φ_g (resp. Φ_h) denote the corresponding solution of (M_g, ∇_g) (resp. (M_h, ∇_h)) (Notation 2.10).

Let $\pi : Y \to X$ be a cover of curves over k and P be a k-rational point of X. We say that P is *completely split* if P is unbranched and every point Q of Y with $\pi(Q) = P$ is k-rational. We now determine a set $\mathfrak{T}$ of completely split places of $\mathcal{T}_{g,h}$.

Define

$$T := \{a \in X_{-1} \mid \mathrm{ord}_a\Phi \not\equiv 0 \bmod p \text{ and } a \notin S\}. \tag{7}$$

Recall that Proposition 2.5 implies that $\mathrm{ord}_a\Phi \equiv 1 \bmod p$ for $a \in T$. The following lemma gives some properties of this set. It will be useful in the investigation of the number of rational points in the tower.

Lemma 3.4. *Suppose Assumption 3.2 holds. Then $\mathfrak{T} := g^{-1}(T) = h^{-1}(T)$.*

Proof. Define $\mathfrak{T} := g^{-1}(T)$. Then $\mathfrak{T} = \{\alpha \in X_0 \,|\, \mathrm{ord}_\alpha(\Phi_g) \not\equiv 0 \bmod p\}$, since $\mathrm{ord}_\alpha(\Phi_g) = \mathrm{ord}_{g(\alpha)}\Phi$ for $\alpha \notin \mathfrak{S}$. Let $\alpha \in \mathfrak{T}$. Proposition 2.12 implies that $\mathrm{ord}_\alpha(\Phi_h) \not\equiv 0 \bmod p$. Therefore $\mathfrak{T} \subset h^{-1}(T)$. The other inclusion is similar. $\square$

Let $\alpha, \beta \in X_0$ with $g(\alpha) = h(\beta)$. Lemma 3.4 shows that $\alpha \in \mathfrak{T}$ if and only if $\beta \in \mathfrak{T}$.

Given a smooth absolutely irreducible curve C defined over $\mathbb{F}_q$, we denote by $N_q(C)$ the number of $\mathbb{F}_q$-rational points of C. For a tower $\mathcal{T}_{g,h} = (X_0, X_1, \dots)$ defined as above with constant field $\mathbb{F}_q$ we define the *splitting rate* of the tower $\mathcal{T}_{g,h}$ by

$$\nu_q(\mathcal{T}_{g,h}) := \lim_{m\to\infty} \frac{N_q(X_m)}{\delta^m}.$$

This limit exists [GST97] and is a nonnegative finite number.

Definition 3.5. Given a correspondence $(g, h) : X_0 \rightrightarrows X_{-1}$ defining a tower $\mathcal{T}_{g,h}$, we define the *minimal splitting field* of this tower to be the smallest field k such that

i) the correspondence $(g, h) : X_0 \rightrightarrows X_{-1}$ is defined over k,

ii) all points of X_0 in the set $\mathfrak{T}$ are defined over k.

A necessary condition for a tower $\mathcal{T}$ to be asymptotically good is $\nu_q(\mathcal{T}) > 0$. The following proposition gives an estimate for $\nu_q(\mathcal{T})$ in our situation.

Proposition 3.6. *Suppose Assumption 3.2 holds. Let $\mathbb{F}_q$ be the minimal splitting field of $\mathcal{T}_{g,h}$. Then*

$$\nu_q(\mathcal{T}_{g,h}) \geqslant \#\mathfrak{T}.$$

Proof. Recall that $\delta := \deg g = \deg h$. Since S and T are disjoint, for any $a \in T$ there are exactly δ points of X_0 lying above a. Moreover, all these points of X_0 are defined over $\mathbb{F}_q$ by our assumption. Let α be a point of X_0 with $g(\alpha) = a$. Write $h(\alpha) = b$. Since $T = g(\mathfrak{T}) = h(\mathfrak{T})$ it follows that $b \in T$.

Now suppose that we have constructed inductively $\delta^{m-1}\#\mathfrak{T}$ points of X_{m-1} defined over $\mathbb{F}_q$ and lying above $\mathfrak{T}$. Let $P \in X_{m-1}$ be one of these points, and let $Q \in \pi_m^{-1}(P) \subset X_m$. Note that the cardinality of $\pi_m^{-1}(P)$ is δ, since P is unbranched in π_m. By assumption, $x_i(P) \in \mathfrak{T}$. Since $h(x_m(Q)) = g(x_{m-1}(Q)) = g(x_{m-1}(P))$, we conclude as above that $x_m(Q) \in \mathfrak{T}$ as well. $\square$

The following theorem gives a sufficient condition for $\mathcal{T}_{g,h}$ to be asymptotically good.

Theorem 3.7. *Suppose Assumption 3.2 holds. Suppose that T is nonempty. Then the tower $\mathcal{T}_{g,h}$ is asymptotically good (with respect to the minimal splitting field $\mathbb{F}_q$).*

Proof. By Proposition 3.3, the tower has finite genus. The assumption implies that $\mathfrak{T} = g^{-1}(T)$ is nonempty. By Proposition 3.6, the tower has positive splitting rate. Therefore the tower $\mathcal{T}_{g,h}$ is asymptotically good. $\square$

Theorem 3.8. *Suppose Assumption 3.2 holds. Let $\mathbb{F}_q$ be the minimal splitting field of $\mathcal{T}_{g,h}$. Suppose that*

$$2\#\mathfrak{T} = (\sqrt{q} - 1)(\#\mathfrak{S} + 2g(X_0) - 2).$$

Then the tower $\mathcal{T}_{g,h}$ is asymptotically optimal.

Proof. This follows immediately from Propositions 3.3 and 3.6. $\square$

The minimal splitting field is in practice often difficult to calculate. This is a serious problem in finding asymptotically optimal towers via the criterion of Theorem 3.8. Proposition 3.9 is a useful tool to deal with this problem: it essentially controls the minimal splitting field at the cost of introducing a new condition on the correspondence $(g,h) : Y \rightrightarrows X$. Namely, we need to suppose that the correspondence has degree one. In Section 4 we will always make this assumption. In the case of modular curves (Section 5) this condition is always satisfied, see the proof of Lemma 5.3.

Recall from Section 2 that if a correspondence $(g,h) : Y \rightrightarrows X$ has degree one, then the map $Y \to C$ of Y onto the curve of correspondence is generically a bijection.

Proposition 3.9. *Let X and Y be smooth and absolutely irreducible curves defined over k, and let $(g,h) : Y \rightrightarrows X$ be a tame correspondence of degree one over k.*

Let $V \subset X$ be a set of k-rational points such that for any $\alpha, \beta \in Y$ with $h(\beta) = g(\alpha)$ we have $g(\alpha) \in V \Leftrightarrow g(\beta) \in V$. Let $\alpha \in Y$ be such that

i) $g(\alpha) \in V$.

ii) $g(\alpha)$ is a k-rational point of X.

iii) $(g(\alpha), h(\alpha))$ is not a singularity of C.

Then α is a k-rational point of Y.

Proof. We first show that $h(\alpha)$ is a k-rational point of X. There exists a point β such that $h(\alpha) = g(\beta)$. By the assumption on V and i), the point $h(\alpha) = g(\beta)$ is in V and hence k-rational.

Since the map ϕ has degree one, it can be inverted for nonsingular points of C. The k-rationality of $(g(\alpha), h(\alpha))$ then implies the k-rationality of $\alpha = \phi^{-1}(g(\alpha), h(\alpha))$. □

Condition iii) in the above lemma is in practice not a heavy restriction. Since the number of singularities of C is finite, they can usually be dealt with by hand in any particular case. For certain correspondences of degree two this lemma is due to Zieve ([GSR03]). We will apply this lemma in the situation that $V = T(= g(\mathfrak{T}) = h(\mathfrak{T}))$. If the conditions of the above lemma are satisfied, then the points in the set $\mathfrak{T}$ are defined over k if the points in the set T are.

4. Constructing towers via pull back

As before let $(g,h) : X_0 \rightrightarrows X_{-1}$ be a correspondence adapted to a Fuchsian differential equation (M, ∇), where we suppose that g and h are disjoint. As always, we suppose that (M, ∇) is cyclic and of order 2. We write S for the set of singularities of (M, ∇). Let $f : Y_{-1} \to X_{-1}$ be a (separable) cover of smooth, absolutely irreducible curves, which is allowed to have wild ramification and may be ramified outside S. We suppose that all curves and covers are defined over a finite field k. Write (M_f, ∇_f) for the pull back of (M, ∇) via f and S_f for the set of singularities of (M_f, ∇_f). In this section we make the following additional assumption.

(f) The correspondence $(g,h) : X_0 \rightrightarrows X_{-1}$ has degree one.

Recall that we defined the curve of correspondence $C \subset X_{-1} \times X_{-1}$ by

$$C := \{(g(P), h(P)) \,|\, P \text{ a point of } X_0\}. \tag{8}$$

The curve C is the image of X_0 under the map $g * h : X_0 \to X_{-1} \times X_{-1}$ defined by $(g * h)(P) = (g(P), h(P))$. Assumption (f) implies that the map $X_0 \to C$ has degree one. Denote by p_1 (resp. p_2) the projections of C onto it first (resp. second) coordinate. We have the following commutative diagram

$$\begin{tikzcd} & X_0 \arrow[dl, "g"'] \arrow[d, "g*h"] \arrow[dr, "h"] & \\ X_{-1} & C \arrow[l, "p_1"] \arrow[r, "p_2"'] & X_{-1}. \end{tikzcd}$$

Let $D \subset Y_{-1} \times Y_{-1}$ be an absolutely irreducible component of the inverse image of C under $(f,f) : Y_{-1} \times Y_{-1} \to X_{-1} \times X_{-1}$. After extending the field of definition k, we may suppose that D is defined over k. We have the following diagram

$$\begin{tikzcd}
 & X_0 \arrow[d, "g*h"] & & & D \arrow[dlll, "{(f,f)}"'] \arrow[dl, "\tilde{p}_1"] \arrow[dr, "\tilde{p}_2"] & \\
 & C \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & & Y_{-1} \arrow[dlll, "f"'] & & Y_{-1} \arrow[dlll, "f"'] \\
X_{-1} & & X_{-1}. & & &
\end{tikzcd}$$

The maps $\tilde{p}_1$ (resp. $\tilde{p}_2$) are projections of D onto its first (resp. second) coordinate. Recall that we always suppose that the curve X_0 is smooth. Denote by Y_0 the normalization of the curve D, then we have the following diagram

$$\begin{tikzcd}
 & Y_0 \arrow[dl, "\tilde{g}"'] \arrow[d] \arrow[dr, "\tilde{h}"] & \\
Y_{-1} & D \arrow[l, "\tilde{p}_1"] \arrow[r, "\tilde{p}_2"'] & Y_{-1}.
\end{tikzcd}$$

The maps $\tilde{g}$ and $\tilde{h}$ are defined such that the diagram commutes.

Definition 4.1. We call $(\tilde{g}, \tilde{h})$ the *pull back* of (g,h) under f.

The following lemma gives a key property of the pull back correspondence $(\tilde{g}, \tilde{h})$.

Lemma 4.2. *The correspondence $(\tilde{g}, \tilde{h})$ is adapted to (M_f, ∇_f).*

Proof. We have the following (commutative) diagram

$$\begin{tikzcd}
 & & & & Y_0 \arrow[dlll, "\phi"'] \arrow[dl, "\tilde{g}"] \arrow[dr, "\tilde{h}"] & \\
 & X_0 \arrow[dl, "g"'] \arrow[dr, "h"] & & Y_{-1} \arrow[dlll, "f"'] & & Y_{-1} \arrow[dlll, "f"'] \\
X_{-1} & & X_{-1}. & & &
\end{tikzcd}$$

Hence the result follows immediately from Lemma 2.13. ☐

Note that if $\deg g = \deg h$, then $\deg \tilde{g} = \deg \tilde{h}$. The above lemma motivates that if the tower $\mathcal{T}_{g,h}$ is asymptotically good, the tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is a good candidate for being asymptotically good as well. Recall that we defined in Lemma 3.4 a set $\mathfrak{T} \subset X_0$ consisting of completely splitting places of the tower $\mathcal{T}_{g,h}$.

Theorem 4.3. *Let (M, ∇) be a Fuchsian differential equation of rank 2 and let (g,h) be a correspondence adapted to (M, ∇) all defined over a finite field $\mathbb{F}_q$. Suppose assumptions (a)–(f) hold. Let $f : Y_{-1} \to X_{-1}$ be a tame cover and suppose that assumption (c) holds for the pull back correspondence $(\tilde{g}, \tilde{h})$ as well. If the set $\mathfrak{T}$ is non empty, then $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically good over some finite extension field of $\mathbb{F}_q$.*

Proof. Our assumptions imply that the branch locus of the pull back tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is contained in $\phi^{-1}(\mathfrak{S})$, where $\phi : Y_0 \to X_0$ is induced by $(f,f) : D \to C$. Therefore Proposition 3.3 implies that the genus $g(\mathcal{T}_{\tilde{g},\tilde{h}})$ of the pull back tower is finite.

We claim that $\nu_q(\mathcal{T}_{\tilde{g},\tilde{h}}) > 0$. By Proposition 3.6, it suffices to show that the set

$$T_f := \{a \in Y_{-1} \,|\, \mathrm{ord}_a \Phi_f \not\equiv 0 \bmod p \text{ and } a \notin f^{-1}(S)\}$$

is nonempty. Let $b \in Y_{-1} - f^{-1}(S)$. Then $\mathrm{ord}_b \Phi_f = e \cdot \mathrm{ord}_{f(b)} \Phi$, where e is the ramification index of b in f. Since f is tamely ramified it follows that $f^{-1}(T) \subset T_f$. Therefore the assumption that T is nonempty implies that T_f is nonempty. $\square$

Before proceeding, we give an example illustrating Theorem 4.3.

Example 4.4. We consider the correspondence $(g,h) : \mathbb{P}^1 \rightrightarrows \mathbb{P}^1$ given by $h(t) = t^2$ and $g(t) = 4t/(t+1)^2$. The correspondence (g,h) is adapted to the Gauß' hypergeometric differential operator $L(u) = t(t-1)u'' + (2t-1)u' + u/4$, which has the Deuring polynomial as a solution (Example 2.6). We denote the Deuring polynomial by Φ. Recall that $S = \{0, 1, \infty\}$ is the set of singularities of L. The set of singularities of the pull back differential equation L_g equals $\mathfrak{S} = \{0, \pm 1, \infty\}$. Therefore the correspondence satisfies assumptions (b) and (d). One checks that the point $x_0 = 0$ on X_0 is totally branched in the tower $\mathcal{T}_{g,h}$. Therefore assumption (c) follows from Lemma 3.1.

The tower $\mathcal{T}_{g,h}$ is the tower of modular curves $X_0(2^m)$ starting from $m = 3$. The tower $\mathcal{T}_{g,h}$ is essentially the same as a tower considered in [GSR03].

The curve of correspondence $C = \{(g(x), h(x)) \,|\, x \in \mathbb{P}^1\}$ is given by the equation

$$4a(b-2)^2 - (a+1)^2 b^2 = 0. \tag{9}$$

One checks that X_0 is a normalization of C. In other words, assumption (f) is satisfied. This means that we can apply the pull back construction to the tower $\mathcal{T}_{g,h}$. Further note that the point $(-1, 2)$ of C is a singularity.

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be the cover defined by $t = f(s) := -n(n/(n-1))^{n-1}(s^n - s^{n-1})$ for an integer $n \geqslant 2$ satisfying $p \not| (n-1)$ and $p \not| n$, where p denotes the characteristic. In particular $Y_{-1} = \mathbb{P}^1$. An explicit calculation shows that the cover f is unbranched outside the set $\{0, 1, \infty\}$. Let $\mathbb{F}_q$ be the smallest finite field containing all roots of the polynomial $\Phi(T^m - T^{m-1})$. Using Proposition 3.9 one checks that the pull back tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically good over the field $\mathbb{F}_q$, for all n for which assumption (c) holds. We will not determine the field $\mathbb{F}_q$ explicitly here. For $n = 2$ we obtain an asymptotically optimal tower which turns out to be the modular tower $((X_0(2^m))$ starting from $m = 4$. For $n > 2$ one does not seem to obtain asymptotically optimal towers. Trivially one sees that q divides $2 \cdot n!$.

Example 4.4 illustrates how to find asymptotically good towers via pull back. The only problem is to check assumption (c) for the pull back tower. This condition is satisfied if $\deg(\tilde{g}) = \deg(g)$. To obtain asymptotically optimal towers, we need to impose a condition on the minimal splitting field. This condition is in practice hard to check.

Theorem 4.5. *Let $(g,h) : X_0 \rightrightarrows X_{-1}$ be a correspondence adapted to a differential equation (M, ∇) with singularity set S, satisfying assumptions (a)–(f). Let $f : Y_{-1} \to X_{-1}$ be a tame cover unbranched outside S. Denote by $(\tilde{g}, \tilde{h})$ the pull back correspondence and suppose it satisfies assumption (c). If $\mathcal{T}_{g,h}$ is asymptotically optimal and the towers $\mathcal{T}_{g,h}$ and $\mathcal{T}_{\tilde{g},\tilde{h}}$ have the same minimal splitting field $\mathbb{F}_q$, then $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically optimal also.*

Proof. By our assumptions $\phi^{-1}(\mathfrak{T})$ consists of completely splitting places of the tower $\mathcal{T}_{\tilde{g},\tilde{h}}$. Therefore $\nu_q(\mathcal{T}_{\tilde{g},\tilde{h}}) \geqslant \deg \phi \cdot \#\mathfrak{T}$ by Proposition 3.6.

As usual, denote by $\mathfrak{S}$ the singularities of the differential equation (M_g, ∇_g). The Riemann-Hurwitz genus formula for the cover $\phi : Y_0 \to X_0$ implies

$$2g(Y_0) - 2 + \#\phi^{-1}(\mathfrak{S}) = \deg \phi \cdot (2g(X_0) - 2 + \#\mathfrak{S}).$$

Since $\phi^{-1}(\mathfrak{S})$ contains the set of singularities of $(M_{\tilde{g}\circ f}, \nabla_{\tilde{g}\circ f})$, it follows from Proposition 3.3 that $g(\mathcal{T}_{\tilde{g},\tilde{h}}) \leqslant \deg\phi \cdot (g(X_0) + (\#\mathfrak{S} - 2)/2)$. This implies the theorem $\square$

As a consequence of Theorem 4.5, we give an asymptotically optimal tower. We consider again the correspondence $(g, h) : \mathbb{P}^1 \rightrightarrows \mathbb{P}^1$ given by $h(t) = t^2$ and $g(t) = 4t/(t+1)^2$. Using Proposition 3.9 we immediately obtain that the roots of the Deuring polynomial are squares in $\mathbb{F}_{p^2}$. In fact these roots are fourth powers in $\mathbb{F}_{p^2}$ (see [GSR03]).

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be defined by

$$t = f(s) = \frac{16s^2}{(s-1)^4}.$$

One checks that $S_f = f^{-1}\{0, 1, \infty\} = \{0, \pm 1, 3 \pm \sqrt{2}, \infty\}$. The pull back differential equation is

$$L_f(v) = v'' + \frac{s^4 - 4s^3 + 20s^2 + 8s - 1}{s(s^2-1)(s^2-6s+1)}v' + \frac{16(s^2+1)}{s(s+1)(s-1)^2(s^2-6s+1)}v = 0.$$

The pull back of C with respect to the map (f, f) has two absolutely irreducible components of genus 0 and one of genus 2. We write $f(A) = a$ and $f(B) = b$ and use (9). The components of genus 0 of the pull back of C are then given by the equations

$$-A + A^2 + 4AB + B^2 - AB^2 = 0 \qquad \text{and} \qquad 1 - A + 4AB - AB^2 + A^2B^2 = 0. \tag{10}$$

One may choose any genus 0 component D from (10) and a coordinate y of its normalization Y_0 such that the maps $\phi : Y_0 \to X_0$ and $\tilde{g}, \tilde{h} : Y_0 \to \mathbb{P}^1$ are described as follows.

$$\begin{tikzcd}
 & X_0 \arrow[dl, "g"'] \arrow[dr, "h"] & & & Y_0 \arrow[lll, "\phi"'] \arrow[dl, "\tilde{g}"'] \arrow[dr, "\tilde{h}"] & \\
\mathbb{P}^1 & & \mathbb{P}^1 & \mathbb{P}^1 & & \mathbb{P}^1,
\end{tikzcd}$$

with $\phi(y) = 4y^2/(y^2-1)^2$, $\tilde{h}(y) = y^2$ and $\tilde{g}(y) = -y(y-1)/(y+1)$.

Let $\mathcal{T}_{\tilde{g},\tilde{h}} = (Y_0, Y_1, \ldots, Y_m, \ldots)$ be the tower of curves defined by the correspondence $(\tilde{g}, \tilde{h})$. One checks that $y_0 = \infty$ is totally branched in the tower. Therefore Lemma 3.1 implies that the curves Y_m are irreducible for all m. Then Y_m is given by the equations

$$y_i^2 = -\frac{y_{i-1}(y_{i-1}-1)}{y_{i-1}+1}, \text{ with } 1 \leqslant i \leqslant m.$$

We write $\Phi_f(s) = \Phi(f(s))$ for the algebraic solution of $L_f(v) = 0$ (Notation 2.10). Using that the correspondence $(\tilde{g}, \tilde{h})$ is adapted to L_f (Lemma 4.2), one checks that

$$(s^2-1)^{2p-2}\Phi_f(s^2) = (s^2+1)^{2p-2}\Phi_f\left(\frac{-s(s-1)}{s+1}\right).$$

This illustrates Proposition 2.12.

PROPOSITION 4.6. *The tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically optimal if* $p \equiv \pm 1 \bmod 8$.

Proof. To apply Theorem 4.5, we only need to determine the minimal splitting field of the tower $\mathcal{T}_{\tilde{g},\tilde{h}}$. Using Proposition 3.9 we see that this field is in fact the splitting field of $\Phi_f(t)$. In other words, we are interested in the solutions of the equation

$$\frac{16y^2}{(y-1)^4} = \left(\frac{4y}{(y-1)^2}\right)^2 = \lambda \text{ with } \Phi(\lambda) = 0. \tag{11}$$

We have already seen that all roots of the Deuring polynomial are squares in $\mathbb{F}_{p^2}$. Write $\lambda = \mu^2$. Equation (11) has solutions in $\mathbb{F}_{p^2}$ if and only if $\mu + 1$ is a square in $\mathbb{F}_{p^2}$.

Suppose that $p \equiv \pm 1 \bmod 8$. We claim that for any root λ of Φ and any element μ with $\mu^2 = \lambda$ the element $\mu + 1$ is a square in $\mathbb{F}_{p^2}$. We will prove this claim following the approach by Rück in the appendix of [GSR03].

Consider the elliptic curve E_λ given by $Y^2 = X(X-1)(X-\lambda)$. Since λ is a root of the Deuring polynomial, E_λ is supersingular. We first suppose that $\lambda \notin \{-1, 2, 1/2\}$ and that λ is not a sixth root of unity. It is known that Frob_{p^2}, the Frobenius automorphism over $\mathbb{F}_{p^2}$, acts on E_λ as multiplication by $\pm p$. This implies that the x-coordinate of any 8-torsion point of E_λ is an element of $\mathbb{F}_{p^2}$. Here we use that $p \equiv \pm 1 \bmod 8$.

The point $(0,0)$ of E_λ is a point of order two. For any point (a,b) satisfying $2(a,b) = (0,0)$ we have

$$a^2 = \lambda$$

as can be seen directly from the addition formulas of E_λ. Hence we may choose $a = -\mu$. For the points (c,d) satisfying $2(c,d) = (a,b)$ we find in a similar way $(c-a)^4 + 4c^2(a-1)^2 a = 0$. Write $\mu = \nu^2$. Note that $\nu \in \mathbb{F}_{p^2}$, since all roots of Φ are fourth powers in $\mathbb{F}_{p^2}$. We obtain

$$(c^2 + 2(-\nu + \mu - \nu\mu)c + \lambda)(c^2 + 2(\nu + \mu + \nu\mu)c + \lambda) = 0. \tag{12}$$

The discriminant of any of these factors is $\mu + 1$ up to multiplication with squares in $\mathbb{F}_{p^2}$. Since all solutions of (12) are in $\mathbb{F}_{p^2}$, the claim follows.

If $\lambda \in \{-1, 2, 1/2\}$, then a direct computation shows that $\mu + 1$ is a square in $\mathbb{F}_{p^2}$ in our situation. On the other hand if λ is a sixth root of unity, then Frob_{p^6}, the Frobenius automorphism on $\mathbb{F}_{p^6}$, acts as multiplication by $\pm p$ on E_λ. By a similar argument as above, we conclude that $\sqrt{\mu+1} \in \mathbb{F}_{p^6}$. On the other hand, it is obvious that $\sqrt{\mu+1} \in \mathbb{F}_{p^8}$. Therefore, $\mu + 1$ is a square in $\mathbb{F}_{p^2}$ in this case as well.

Theorem 4.5 now implies that the tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically optimal. The tower $\mathcal{T}_{\tilde{g},\tilde{h}}$ is asymptotically good (though not optimal) for every $p > 2$ if we extend the field of definition to $\mathbb{F}_{p^4}$. $\square$

5. Towers of modular curves

In this section we apply the results of Sections 3 and 4 to towers of modular curves.

Fix an integer $\ell > 3$. We do not suppose that ℓ is prime. Write $X_0(\ell^m)$ for the modular curve parameterizing (generalized) elliptic curves E together with a cyclic isogeny $E \to E'$ of degree ℓ^m. For a precise description of the points above $j = \infty$ (the cusps) in terms of generalized elliptic curves we refer to [DR72]. The curve $X_0(\ell^m)$ has a natural smooth model over $\mathbb{Z}[1/\ell]$. Denote by $\sigma_m : X_0(\ell^m) \to X_0(\ell^m)$ the Atkin–Lehner involution. It sends an isogeny $E \to E'$ to its dual isogeny.

We define a correspondence $(g,h) : X_0(\ell^2) \rightrightarrows X_0(\ell)$ as follows. Suppose that $(E_1 \to E_2 \to E_3)$ corresponds to a point of $X_0(\ell^2)$, i.e. $E_1 \to E_3$ is a cyclic isogeny of degree ℓ^2 and $E_i \to E_{i+1}$ has degree ℓ. Then $g(E_1 \to E_2 \to E_3) = (E_1 \to E_2)$ is the standard projection and $h(E_1 \to E_2 \to E_3) = (E_2 \to E_3)$ is $\sigma_1 \circ g \circ \sigma_2$.

Analogous to Example 2.6, we obtain a differential equation on $X_0(\ell^m)$. Fix a prime p relatively prime to ℓ. We denote by $X_0(\ell^m)/\mathbb{F}_p$ the reduction of $X_0(\ell^m)$ to characteristic p.

Let $S = \mathrm{Spec}(\mathbb{F}_p[j, 1/j(j-1728)])$. Write $\mathcal{E}_{\ell^m}$ for the universal elliptic curve on $X_0(\ell^m)$; it exists for $\ell^m > 3$. Let $M_{\ell^m} = H^1_{\mathrm{dR}}(\mathcal{E}_{\ell^m}/S)$ be the de Rham cohomology group and $\nabla : M_{\ell^m} \to \Omega^1_S \otimes M_{\ell^m}$ the Gauß–Manin connection ([Kat70, Section 7]). Then $(M_{\ell^m}, \nabla) \in \mathrm{MC}(X_0(\ell^m))$; its set of singularities S_{ℓ^m} is contained in the inverse image of $j = 0, 1728, \infty$.

Lemma 5.1. *The correspondence $(g,h) : X_0(\ell^2) \rightrightarrows X_0(\ell)$ is adapted to (M_ℓ, ∇).*

Proof. The pull back of $\mathcal{E}_\ell$ via g is just the universal elliptic curve $\mathcal{E}_{\ell^2}$. Denote the pull back of $\mathcal{E}_\ell$ via

h by $\mathcal{E}'_{\ell^2}$. The concrete description of g and h given above implies that there is an isogeny $\mathcal{E}_{\ell^2} \to \mathcal{E}'_{\ell^2}$. It induces an isomorphism $H^1_{\mathrm{dR}}(\mathcal{E}_{\ell^2}/S) \simeq H^1_{\mathrm{dR}}(\mathcal{E}'_{\ell^2}/S)$ on the de Rham cohomology groups. This implies the statement of the lemma. $\square$

On $X(1)$ we still have a versal family of elliptic curves $\mathcal{E}_1$. We may choose $\mathcal{E}_1$ such that it is nonsingular outside $j = 0, 1728, \infty$. The differential equation corresponding to (M_1, ∇) is a hypergeometric differential equation (i.e. a Fuchsian differential equation with three singularities). Its singularities are $j = 0, 1728, \infty$ with local exponents $0, 1/3; 0, 1/2; 1/12, 1/12$, respectively. Note that (M_{ℓ^m}, ∇) is the pull back of (M_1, ∇) via the natural projection $(E \to E') \mapsto E$. Denote by $\nu_2(\ell^m)$ (resp. $\nu_3(\ell^m)$, resp. $\nu_\infty(\ell^m)$) the number of singularities of (M_{ℓ^m}, ∇) above $j = 1728$ (resp. $j = 0$, resp. $j = \infty$). Let $\mu(\ell^m)$ be the degree of $X_0(\ell^m) \to X(1)$. These numbers are computed in [Shi94, Proposition 1.43]. Moreover, it is shown in [Shi94, Proposition 1.40] that

$$g(X_0(\ell^m)) = 1 + \frac{\mu(\ell^m)}{12} - \frac{\nu_2(\ell^m)}{4} - \frac{\nu_3(\ell^m)}{3} - \frac{\nu_\infty(\ell^m)}{2}. \tag{13}$$

The *supersingular polynomial* is defined as

$$\Phi_1(j) = \prod (j - j(E)) \in \mathbb{F}_p[j],$$

where the product is taken over the supersingular elliptic curves $E/\bar{\mathbb{F}}_p$. Put

$$\alpha := \left[\frac{p}{12}\right], \quad \delta := \begin{cases} 0 & \text{if } p \equiv 1 \bmod 3 \\ 1 & \text{if } p \equiv 2 \bmod 3 \end{cases}, \quad \epsilon := \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4 \\ 1 & \text{if } p \equiv 3 \bmod 4 \end{cases}.$$

There exists a polynomial $\tilde{\Phi}_1$ of degree α such that $\Phi_1 = j^\delta (j - 1728)^\epsilon \tilde{\Phi}_1$. All zeros of $\tilde{\Phi}_1$ are simple.

Lemma 5.2. *The polynomial $\tilde{\Phi}_1$ is an algebraic solution of* (M_1, ∇).

Proof. This is well known. It can for example be checked by direct verification, or deduced from [Kat84]. $\square$

We denote by $\tilde{\Phi}_{\ell^m}$ the induced algebraic solution of $(M_{\ell^m}, \nabla) \otimes \mathbb{F}_p$ (Notation 2.10).

Lemma 5.3. *We write*

$$T_\ell := \{x \in X_0(\ell)_{\mathbb{F}_p} \,|\, \tilde{\Phi}_\ell(x) = 0, \text{ and } x \notin S_\ell\}.$$

The points of T_ℓ are $\mathbb{F}_{p^2}$-rational.

Proof. It is well-known that the roots of $\tilde{\Phi}_1$ are rational over $\mathbb{F}_{p^2}$ ([Sil86]).

For $j_1, j_2 \in X(1)$ we write $j_1 \sim_\ell j_2$ if there exists a cyclic isogeny of degree ℓ from the elliptic curve with j-invariant j_1 to the elliptic curve with j-invariant j_2. Define a (singular) curve

$$\mathcal{C}(\ell) = \{(j_1, j_2) \in X(1) \times X(1) \,|\, j_1 \sim_\ell j_2\}.$$

We obtain a commutative diagram

$$\begin{tikzcd}
& X_0(\ell) \arrow[d] \arrow[ddl, "g_0"'] \arrow[ddr, "h_0"] & \\
& \mathcal{C}(\ell) \arrow[dl, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \\
X(1) & & X(1),
\end{tikzcd}$$

with $g_0(E_1 \to E_2) = j(E_1)$ and $h_0(E_1 \to E_2) = j(E_2)$ (compare to (8)).

If E_1 and E_2 are elliptic curves with $j \neq 0, 1728$, there exists at most one isogeny $E_1 \to E_2$ of fixed degree ℓ. Namely, let $\varphi_1, \varphi_2 : E_1 \to E_2$ be two cyclic isogenies of the same degree. Then they differ by an authomorphism ψ of E_1. But since $j(E_1) \neq 0, 1728$ it follows that ψ is $\pm I$. This implies that the map $X_0(\ell) \to \mathcal{C}(\ell)$ has degree one and is defined over $\mathbb{F}_p$. The lemma now follows from Proposition 3.9, since the roots of Φ_1 are $\mathbb{F}_{p^2}$-rational. □

Proposition 5.4. *Let $\ell > 3$ be an integer.*

i) Let $(g, h) : X_0(\ell^2) \rightrightarrows X_0(\ell)$ be the correspondence defined above. Then the corresponding tower of curves is isomorphic to $\mathcal{T}_{g,h} = (X_0(\ell^m))$.

ii) The tower $\mathcal{T}_{g,h}$ is asymptotically optimal.

Proof. Part i) is proved in [Elk98]. Part ii) follows from the work of [Iha99]. It is also proved in [TVZ82]. We indicate an alternative proof using our results.

If $\nu_2(\ell^2) = \nu_3(\ell^2) = 0$, the proposition follows from Theorem 3.8. Otherwise, the estimates for $g(X_0(\ell^m))$ and $N_{p^2}(X_0(\ell^m))$ given in Section 3 are not quite good enough. But it is easy to compute these quantities directly, using the results of [Shi94]. Namely, one checks that

$$\lim_{m\to\infty} \frac{\nu_2(\ell^{m+1})}{\delta^m} = \lim_{m\to\infty} \frac{\nu_3(\ell^{m+1})}{\delta^m} = \lim_{m\to\infty} \frac{\nu_\infty(\ell^{m+1})}{\delta^m} = 0.$$

Therefore (13) implies that the genus of the tower is

$$\lim_{m\to\infty} \frac{g(X_0(\ell^{m+1}))}{\delta^m} = \frac{\mu(\ell)}{12}. \tag{14}$$

To estimate the splitting rate in the tower, one needs to count the points on $X_0(\ell^m)$ above $j = 0, 1728$ which are not singularities. Such points above $j = 0$ (resp. $j = 1728$) are zeros of the pull back of Φ if and only if $j = 0$ (resp. $j = 1728$) is supersingular, i.e. $p \equiv 2 \bmod 3$ (resp. $p \equiv 3 \bmod 4$). Distinguishing cases according to the value of $p \bmod 12$, one finds that

$$\lim_{m\to\infty} \frac{N_{p^2}(X_0(\ell^{m+1}))}{\delta^m} \geqslant \frac{(p-1)\mu(\ell)}{12}. \tag{15}$$

Equations (14) and (15) imply that the tower is optimal. □

It is easy to see that for every $a \geqslant 1$ we can consider the tower defined by the correspondence $(g, h) : X_0(\ell^{a+1}) \rightrightarrows X_0(\ell^a)$. This yields the subtower $(X_0(\ell^{a+m}))$ which is of course again asymptotically optimal.

We now present a variant of this construction. Choose an integer λ relatively prime to ℓ and p. Consider the pull back of the correspondence $(g, h) : X_0(\ell^{a+1}) \rightrightarrows X_0(\ell^a)$ via the natural projection $X_0(\lambda\ell^a) \to X_0(\ell^a)$. It is easy to see that the pull back correspondence is $(\tilde{g}, \tilde{h}) : X_0(\lambda\ell^{a+1}) \rightrightarrows X_0(\lambda\ell^a)$.

Proposition 5.5. *The tower defined by $(\tilde{g}, \tilde{h}) : X_0(\lambda\ell^{a+1}) \rightrightarrows X_0(\lambda\ell^a)$ is*

$$\cdots \to X_0(\lambda\ell^m) \to \cdots X_0(\lambda\ell^{a+1}) \to X_0(\lambda\ell^a).$$

This tower is asymptotically optimal.

Proof. This is analogous to the proof of Proposition 5.4. □

We illustrate in an example how easy it is to compute equations for modular curves, by using the recursive definition.

Example 5.6. We want to compute equations for the curve $X_0(2 \cdot 3^m)$ in characteristic $p \neq 2, 3$. Our method is essentially the same as the method of Elkies [Elk98].

Note that the genus of $X_0(18)$ is zero. For $N=3,6,18$, we write $L_N(u)=0$ for the differential equation corresponding to $(H^1_{\mathrm{dR}}(\mathcal{E}_N/S),\nabla)$. Using the description of the cusps in [Shi94], it is easy to check the following statements. The differential equation $L_3(u)=0$ has three singularities. It is no restriction to suppose that these singularities are $x=0,1,\infty$, where ∞ maps to $j=0$ and $x=0,1$ map to $j=\infty$ with ramification index $1,3,1$, respectively. The map $X_0(6)\to X_0(3)$ of degree three is totally branched above $x=\infty$ and has two points P_0^1,P_0^2 (resp. P_1^1,P_1^2) above $x=0$ (resp. $x=1$), where P_*^e is ramified of order e. Up to normalization, there is a unique such cover which is given by $x=-27y^2/(y-4)^3$. It follows that the singularities of $L_6(u)=$ are $S_6=\{0,\infty,-8,1\}$. A look at the ramification indices of these cusps in $X_0(6)\to X(1)$ tells us that the Atkin–Lehner involution σ_6 acts on these points as $(0,1)(-8,\infty)$, therefore $\sigma_6(y)=-8(x-1)/(x+8)$.

A similar argument shows that the natural projection $g:X_0(18)\to X_0(6)$ is cyclic of order three and branched at $y=0,\infty$. Therefore we may suppose that $X_0(18)\to X_0(6)$ is given by $g(z)=z^3$. The singularities of $L_{18}(u)=0$ are just the inverse image of S_6, i.e. $S_{18}=\{0,\infty,-2\zeta_3^i,\zeta_3^i\}$, where $\zeta_3\in\mathbb{F}_{p^2}$ is a primitive third root of unity. The Atkin–Lehner involution is given, up to normalization, by $\sigma_{18}(z)=-2(z-1)/(z+2)$. We define the rational function $h(z)=\sigma_6\circ g\circ\sigma_{18}(z)=z(z^2-2z+4)/(z^2+z+1)$. This gives the recursive definition for the modular curves $X_0(2\cdot 3^m)$.

For λ relatively prime to p, we may define the congruence subgroup $\Gamma_1(\lambda)\cap\Gamma_0(\ell^a)$. Write $X_{1,0}(\lambda,\ell^a)_{\mathbb{C}}$ for the quotient curve of the completed upper half plane by $\Gamma_1(\lambda)\cap\Gamma_0(\ell^a)$. It is well known that $X_{1,0}(\lambda,\ell^a)_{\mathbb{C}}$ has a model $X_{1,0}(\lambda,\ell^a)_R$ over $R=\mathbb{Z}[\zeta_\lambda,1/\lambda\ell]$, where ζ_λ is a primitive λth root of unity. Write $\mathbb{F}_q=\mathbb{F}_p[\zeta_\lambda]$ and $X_{1,0}(\lambda,\ell^a)=X_{1,0}(\lambda,\ell^a)_R\otimes\mathbb{F}_q$. Let $f:X_{1,0}(\lambda,\ell^a)\to X_0(\ell^a)$ be the natural projection.

We can consider the pull back of $(g,h):X_0(\ell^{a+1})\rightrightarrows X_0(\ell^a)$ via $f:X_{1,0}(\lambda,\ell^a)\to X_0(\ell^a)$. Write $\mathcal{T}_{g,h}(f):=(X_{1,0}(\lambda,\ell^{a+n}))$ for the corresponding tower. As in [LMS02], one give a criterion on p for this tower to be asymptotically optimal. For example, the tower of Proposition 4.6 is isomorphic to $(X_{1,0}(8,2^{4+m}))$. It should be possible to give an alternative proof of the facts on the minimal splitting field by using this interpretation of the tower.

References

DR72 P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable II, LNM, no. 349, Springer-Verlag, 1972, pp. 143–316.

DV83 V. G. Drinfel'd and S. G. Vlăduţ, *Number of points of an algebraic curve*, Funct. Anal. **17** (1983), 53–54.

Elk98 N. D. Elkies, *Explicit modular towers*, Proceedings of the 35th annual Allerton conference on communication, control and computing, (Urbana, 1997), 1998, pp. 23–32.

Elk01 N. D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, 2001, pp. 189–198.

Gop81 V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), 1289–1290.

GS95 A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.

GS96 ______, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248–273.

GS00 ______, *Skew pyramids of function fields are asymptotically bad*, Coding theory, cryptography and related areas (Guanajuato, 1998), Springer, 2000, pp. 111–113.

GSR03 A. Garcia, H. Stichtenoth, and H. Rück, *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

GST97 A. Garcia, H. Stichtenoth, and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite fields and their applications **3** (1997), 257–274.

Hon81 T. Honda, *Algebraic differential equations*, Symposia Mathematica, Vol. XXIV (Sympos. INDAM, Rome, 1979), Academic Press, London, 1981, pp. 169–204.

Iha99 Y. Ihara, *Shimura curves over finite fields and their rational points*, Applications of curves over finite fields (Seattle, 1997), Contemp. Math, vol. 245, Amer. Math. Soc., 1999, pp. 15–23.

Kat70 N. M. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. **39** (1970), 175–232.

Kat84 N. M. Katz, *Expansion-coefficients as approximate solution of differential equations*, Astérisque **119-120** (1984), 6, 183–189.

LMS02 W.-C. W. Li, H. Maharaj, and H. Stichtenoth, *New optimal tame towers of function fields over small finite fields*, ANTS–5, LNCS, vol. 2369, Springer, 2002, with an appendix by N. D. Elkies, pp. 372–389.

Ser83 J-P Serre, *Nombres de points des courbes algébriques sur* $\mathbf{F}_q$, Sémin. Théor. Nombres, 1982–1983 (Talence, 1982/1983), Talence, 1983, Exp. No. 22.

Shi94 G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1994.

Sil86 J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, 1986.

TV91 M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Kluwer Academic Publishers Group, 1991.

TVZ82 M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, *Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

Peter Beelen P.Beelen@mat.dtu.dk
Universität Duisburg–Essen, Fachbereich Mathematik, Campus Essen, D-45117 Essen
Current address: Department of mathematics, Danish Technical University, DK-2800 Kgs. Lyngby

Irene I. Bouw bouw@math.uni-duesseldorf.de
Institut für Experimentelle Mathematik, Ellernstraße 29, D-45326 Essen
Current address: Mathematisches Institut, Heinrich-Heine-Universität, D-40225 Düsseldorf